

Blockchain-based Architectures for the Internet of Things: A Survey.

Marcella Atzori, Affiliate Researcher, UCL – Research Center for Blockchain Technologies

Abstract—This research explores the main features of three blockchain-based platforms for the Internet of Things, as recently emerged in academia as well as in industry. If properly engineered, the blockchain technology offers a disruptive solution to the problem of security and privacy in the Internet of Things environment, providing a new computational layer where data can be safely processed and analyzed, remaining private. The blockchain can also enable micro-payment functionality between digitally-enhanced devices, through ultra-light cryptocurrencies and smart contracts. The implementation of such features is expected to ensure a more efficient allocation of resources at global level, however it may also lead to undesirable consequences – such as a hyper-tokenization of society and a potentially dystopian concentration of power on big global platforms. Therefore, overall benefits and drawbacks of the blockchain deployment must necessarily take account of specific contexts of use, finding a balance between need for innovation and social sustainability.

Index Terms—blockchain, cryptocurrency, Internet of Things, privacy, security, smart contracts

I. INTRODUCTION

This paper aims to explore practical applications of blockchain, cryptocurrencies and smart contracts in the Internet of Things context. Section II will provide a general overview of the Internet of Things and blockchain technology, with particular reference to privacy engineering, security and micro-payment functionality.

The next sessions will focus on case studies of blockchain-based platforms, specifically designed for the Internet of Things purposes: *Enigma* (Session III); *IOTA-Tangle* (Session IV); and *ADEPT* (Session V).

In conclusion, we will discuss benefits, drawbacks, and open issues related to the blockchain implementation in the sector, both at a technical and societal level.

II. INTERNET OF THINGS AND BLOCKCHAIN TECHNOLOGY: AN OVERVIEW

A. Defining the Internet of Things

The Internet of Things (IoT) consists of a global network of billions of uniquely identifiable and addressable objects, embedded with transducers (sensors, actuators, controllers) and connected to the Internet in wireless mode. More precisely, the International Telecommunication Union defines the IoT as a “dynamic, global network infrastructure that can self-configure using standards and using interoperable protocols where (physical and virtual) things have identities, attributes, and personalities, use intelligent interfaces, and can seamlessly integrate into the network” [1]. The IoT is both a global physical infrastructure and an all-embracing concept for many existing and evolving interoperable ICTs, services and applications, increasingly deployed in different domains such as industrial control, health care, aviation, home automation, retail, transport, wearables, and more.

There can be many different ways of calling the IoT network, for example *web of things*, *Internet of Everything*, *Cloud* or *Fog network*. All these concepts are very similar and they belong to the same technological paradigm, called *pervasive* or *ubiquitous computing*. First proposed in 1999, this paradigm aims at redefining the whole relationship of humans, work, and technology [2]. It entails computational activities happening *anytime*, *everywhere* and *with any device*, with no or very limited human intervention, through “sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives and connected through a continuous network” [3].

In particular, under the architecture of the IoT, machine-to-machine transactions (M2M) have arisen as a new organizational and business model, in which digitally enhanced devices execute automated and real-time exchange of technological resources like data, computational power, storage, bandwidth, and electricity. The value exchange functionality of devices is expected to bring several benefits and advantages to individuals and society, such as an increased efficiency in the allocation of resources at global level, with possible applications in smart grid, smart home, smart robots, health care, manufacturing systems, and cyber-transportation systems (CTS) [4].

Marcella Atzori (marcella.atzori@gmx.com) is affiliate researcher at University College of London – Center for Blockchain Technologies, Department of Computer Science - Malet Place, WC1E 6BT London, United Kingdom.

B. *IoT main challenges and the growing need for trust*

The wide-spread proliferation of devices gathering data from different environments and engaged in real-time transfer of resources poses major problems in terms of data security, privacy, resilience, storage, and centralization. Some of these risks are known, other unanticipated, but societal vulnerability must always be taken into serious consideration, besides the potential business benefits of such technology [5].

Security flaws in the IoT may lead, for instance, to malicious attacks on secrecy and authentication, silent attacks on service integrity, or attacks on network availability, such as the denial of service (DoS) [6].

Privacy and anonymity, on the other hand, are no less serious issues. The IoT objects are natural “collectors and distributors of information” [7], so they represent a unique challenge to individual privacy [8]. In particular, the ubiquitous interaction of users with smart objects and groups of things; the invisible and automated collection of fine-grained data by third parties; and the uncontrolled concentration of such data on platforms lacking in transparency may systematically expose users to several threats, such as: identification, localization, monitoring, tracking, surveillance, manipulation, profiling, targeted advertising, data linkage, and even social engineering [9] [10]. Such threats, in turn, can result in service inefficiency: citizens, for example, may be refrained from effectively interacting with smart city infrastructures, as a result of a diffused sense of insecurity [7].

The growing concern of academic literature for the IoT has recently prompted a significant number of technical and legal recommendations, with the aim of reducing its harmful effects. *Privacy-by-policy* and *privacy-by-design* have emerged as new approaches to the IoT and the tremendous, unprecedented flow of data it generates—which would require to be thought and treated in itself as *infrastructure* [11]. The aim of *privacy-by-policy* is to protect data from accidental disclosure or misuses, also promoting informed customer choice [12] [13]; instead, *privacy-by-design* focuses on the necessity to implement privacy throughout the engineering process, with a proactive and preventative approach, rather than *ex post* [7] [14].

The combination of these methods has proven fundamental to conceptualize and mitigate potential risks associated with the IoT, which nonetheless remains a highly controversial paradigm. On one side, the IoT globality and ubiquity would require to promote legal safeguards beyond any geographical boundary, preferably through an international legislator [15]; on the other side, regulators still struggle to effectively harmonize different judicial sensitivities at global level, and they can hardly keep up with technological development and markets – which are moving inexorably forward at an astounding pace, but with no clear common standards yet. As a consequence, new

privacy-engineering practices and distributed architectures are increasingly urgent needed to properly address the IoT major challenges.

C. *The blockchain for privacy engineering, security and micro-payments*

The blockchain is a computational paradigm emerged for the first time with the Bitcoin protocol in 2008 [16]. It consists of a distributed ledger which contains all transactions ever executed within its network, enforced with cryptography and carried out collectively by a peer-to-peer workgroup. The blockchain is a trust-free, tamper-proof, auditable, and self-regulating system, with no human intervention required to execute computation. As a secure and decentralized computational infrastructure, it is widely acknowledged as a disruptive solution for the problems of centralization, privacy and security when storing, tracking, monitoring, managing and sharing data.

Based on cryptographic protocols, the blockchain is able to effectively protect integrity, authenticity, auditability and consistency of all transactions. It can hence play a major role in the IoT ecosystem, reducing time- and cost-consuming workflows [17] and providing an architectural layer where data can be processed and analyzed, but remain private or semi-private [18]. In line with the principle of *privacy-by-design*, the blockchain minimizes the need for regulation, and it also makes possible to embed laws in the code, so they can be automatically executed. The blockchain is thus more functional than other complex Privacy-Enhancing Technologies (PET) – which may turn out to be somehow impractical or inefficient [15].

Besides security and privacy protection, the blockchain also enables micro-payments and automated transfer of assets between IoT devices, through cryptocurrencies and smart contracts. Originally introduced by Nick Szabo in 1994 [19], smart contracts consist of scripts stored on a blockchain and visible to every node of the network, containing self-executing agreements between two or multiple parties. They can be run through platforms for decentralized applications such as Ethereum, and when triggered by a transaction, they automatically execute the instructions agreed by participants. Smart contracts are autonomous, decentralized, predictable, and deterministic by their own nature: once launched and running, they need no further action from the parties involved and they are potentially unstoppable [20].

Thanks to their specific features, blockchain, cryptocurrencies and smart contracts may become the seamless and decentralized economic layer of the IoT, ensuring adequate privacy and security to users [18]. To achieve this result, however, the blockchain must be properly designed and this is actually very challenging.

D. Blockchains for the IoT

The first problem is that open, general-purpose blockchains and digital currencies like Bitcoin are generally not suitable for the IoT purposes, since they are too complex, costly, and also suffer from scalability problems and latency of confirmation time (currently 10 minutes in the Bitcoin network). Privacy and confidentiality within such networks are also relative, since transactions are visible to all nodes. A further problem is that the IoT often deals with constrained environments. Devices may have to work with low computational capability, very low power, or lossy networks; they may also be engaged in minimal, but very frequent transmissions of data, which need to be processed in real-time and at low or no fees, especially in case of cost critical markets. Therefore, the IoT requires lightweight blockchain architectures, with no heavy computational power nor obtrusive additional hardware for devices.

The blockchain technology is still at an early stage of development and further research is needed to overcome hurdles of implementation in the IoT environment. Significant contributions, however, have already begun to emerge in academia as well as in industry, with the aim of providing the IoT with security, privacy and micro-payment functionality. We will briefly analyze the key features of three examples which stand out for their potential applications, and we will verify how they address the IoT main challenges.

III. ENIGMA: A BLOCKCHAIN-BASED PLATFORM FOR PERSONAL DATA PROTECTION

Zyskind, Nathan and Pentland have recently developed *Enigma*, a peer-to-peer network based on a decentralized personal data management system, which enables different parties to “jointly store and process computations on data, while keeping the data completely private” [21] [22]. The system guarantees privacy- by-design and correctness, effectively combining blockchain technology and off-chain data storage.

As the developers recalled, current public blockchains are not suitable for heavy computations and privacy protection, because data flow through every node on the blockchain, resulting in being fully exposed. An off-chain solution for data storage is hence more desirable and functional. While such design still requires a minimal trust in the manager, it is essential to ensure scalability, ease of deployment, and privacy itself.

According to developers, Enigma is more secure than others anonymization and privacy-preserving methods, where data can be actually de-anonymized. It is also preferable to fully homomorphic encryption (FHE), currently too inefficient.

The fundamental features of Enigma can be summarized as follows [21] [22].

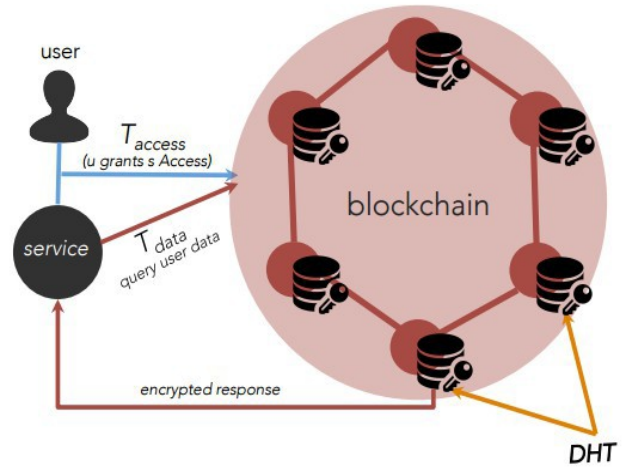


Fig. 1 – ENIGMA: a blockchain-based decentralized platform for IoT privacy – Source: Zyskind, Nathan and Pentland, 2015.

Off-blockchain data storage. Enigma has a privacy-preserving and fault tolerant design. It consists of a decentralized off-chain distributed hash-table (DHT), a private chain of nodes accessible through the blockchain. It stores references to the data, but not the data themselves, which are splitted and randomized. No node has access to entire data.

The blockchain. It operates as a trustless automated access-control manager. It recognizes data owners, provides controlled access to other parties and serves as a tamper-proof log of events.

Privacy-enforcing computation. The distributed computational model of Enigma is based on secure Multi Party Computation (sMPC). Data queries and calculations are processed in a completely distributed way, without the need of a third party: each node performs computation over different parts of the data without decrypting them first and without leaking the data to the nodes. The result is guaranteed through a verifiable secret-sharing scheme.

Off-chain heavy processing. Intensive calculations and analysis on data are performed on the off-chain only. Since transactions are not replicated by every node, the blockchain does not have problems of scalability. The reduced redundancy in storage and computations enables even more intense computations.

Benefits of Enigma for users are significant [21], including:

Data ownership and reward: users own and control their personal data; they can also receive a token as a compensation for the use of their data.

Transparency and auditability: users can monitor what data is being collected, how they are accessed and by who.

Fine-grained access control: users can modify the set of permissions and revoke access to collected data at any time. Traditional mobile applications, on the contrary, require users to agree on a set of permissions, so that they can only opt-out.

Data accessibility and use: interested parties can access and use data, without being concerned at first hand about security. Risks associated with the data management chain will be reduced accordingly.

Minimal regulatory intervention: laws about collecting, storing and sharing sensitive data can be simplified.

Embedded regulation: legal framework can be incorporated and automatically executed through the blockchain code.

Provision of legal evidence: the blockchain ensures integrity of data and provides a tamper-proof log of events, acting as legal evidence for accessing and storing data.

IV. IOTA-TANGLE: A DECENTRALIZED IOT SETTLEMENT SYSTEM

IOTA is a cryptocurrency specifically developed for micro-payments, which aims at becoming a standard settlement system in the IoT and machine-to-machine economy [23]. Beside business-to-business applications, IOTA can be also used for households and wearable devices, for example, allowing users to own and sell their data in real-time, instead of being unwittingly monitored for market analysis [23].

IOTA possible applications are undoubtedly promising. As its creator David Sønstebo pointed out [23], the increasing development of the IoT leads to the emergence of the so-called *Fog* and *Mist*. These computing paradigms decrease the network latency that exists when big cloud data centers are located too far away from the end-devices. In particular, the *Fog* pushes computationally intensive applications to the gateway, while the *Mist* pushes the less computationally intensive tasks to the very edge of the network, namely to the sensors and actuators of the device itself. It is in the *Fog* and *Mist* environment that transactions are expected to grow exponentially, enabling the rising of new business models, products and services. It is hence crucial for the industry to rely on a real-time and decentralized settlement system, at no charge.

IOTA is build on the top of *Tangle* [24], a lightweight blockchain “without blocks” and most importantly with no transaction fees – a key factor to preserve cost-effectiveness. In the words of Sønstebo, “IOTA is currently the only project that solves the issue of scalability and fees without any ad hoc solutions that compromise the integrity of the security or decentral nature of the economy” [23].

The principal characteristics of Tangle architecture are as follows [24]:

- the chain of blocks typical of Bitcoin is replaced by a *tangle* or DAG (directed acyclic graph), namely a collection of nodes that acts as a ledger to store transactions;
- network is asynchronous and transactions are confirmed by direct and indirect approvals of the nodes. No rules are imposed for the approval, only reference rules exist;
- in case of conflicting transactions, a node decides which transaction will be left orphaned through an algorithm that predicts which transaction is more likely to be approved by the network;
- nodes have to solve a demanding mathematical puzzle to verify a transaction and they must propagate it through the network: in case a node is too lazy, it will be dropped by the other peers;
- transactions are not approved in blocks, but individually and at no charge.

Powered by Tangle and quantum-resistant algorithms, IOTA architecture is efficient, scalable, very light, and according to developers, more resistant to security breaches than any other cryptocurrency. Moreover, IOTA is interoperable: it can communicate to other established blockchains such as Bitcoin and Ethereum, providing checkpoints for these networks and reinforcing their ecosystems. Indeed, the intention of developers is not to replace the open blockchains entirely, but to be complementary to the current ecosystem and operate in conjunction with it [25]. Finally, IOTA can also be used as an oracle for smart contracts.

Partnered with Chain Of Things, IOTA will join Azure [23], the Microsoft's blockchain-as-a-service (BaaS) solution for a “certified blockchain marketplace” [26]. Azure is designed as a low-risk sandbox for many technologies and all possible blockchains.

V. IBM & SAMSUNG ELECTRONICS: ADEPT

With the joint research partner Samsung Electronics, IBM has been one of the first IT giants to move towards blockchain solutions for the IoT, with the aim of developing a new business paradigm and vision of the world: the so-called Economy of Things.

In a draft released in January 2015 and titled “ADEPT: An IoT practitioner perspective”, the company proposed a blockchain-based project called ADEPT, namely Autonomous Decentralized Peer-to-Peer Telemetry [27]. The final version of such working paper was later released online as a report titled “Device democracy - Saving the future of the Internet of Things” [28].

IBM recognizes the value of a blockchain-based decentralized approach to the IoT, in order to gain greater

scalability, robustness and security, as well as privacy-by-design. The result is “the Internet of Decentralized, Autonomous Things” [28], a dynamic democracy of objects connected to a universal digital ledger, which provides users with secure identification and authentication. This concept, in IBM vision, is going to shape a brand new model of business in the very next future.

ADEPT architecture is based on TeleHash (as messaging protocol), BitTorrent (as an efficient distribution layer) and Ethereum (as a platform for smart contracts and *Decentralized Autonomous Organizations*) [27]. Its main features can be summarized as follows [27] [28].

A transparent system and a fully distributed proof: transactions are validate through a combination of proof-of-work and proof-of stake.

An architecture suitable for different nodes: the nodes of the network can be distinguished according to their level of computational power and memory:

- *Light Peers* (e.g. Raspberry Pi, Beaglebone, or Arduino boards) have low resources: they can perform messaging and work as light wallets, but they are not able to manage the blockchain, so they obtain the blockchain transactions from other trusted peers.
- *Standard Peers* are equipped with higher storage and processing resources, so to meet blockchain requirements and support Light Peers, according to their capabilities. As costs of chips decline, IBM expects that an increasing number of smart objects will be able to be included in this category of nodes.
- *Exchange or ADEPT Peers* have large memory and computational power, so they are capable to manage and store complete copies of the blockchain. They can host marketplaces and they can be owned by organizations or commercial operators, providing blockchain analytical services and doing complex queries. These nodes represent the core of ADEPT philosophy and the “Silky routes” of a new economical paradigm. Indeed, they can perform the role of financial exchanges across communities, insofar as they are able to balance demand and supply of services, assets and products. They can take into account resources available in a community and find buyers in another, performing the function of “liquification of assets”.

Autonomy of devices: through smart contracts running on Ethereum, devices can autonomously execute payments, agreements, tradings, barter and exchange of resources with other peers. They can also detect possible operational problems and do self-maintenance.

A user-centric model: devices will act in the best interest of

the user, rather than third parties (e.g. manufacturers, governments or service providers).

Blockchain by default: products and devices should be registered by the manufacturer into a universal blockchain, at the beginning of their lifecycle.

ADEPT represents an interesting attempt of the industry to make the IoT ecosystem more sustainable, through a decentralized, peer-to-peer and user-centric approach. The platform, however, still needs to overcome several technical issues, as author [29] pointed out.

Scalability: to manage a global blockchain for the IoT eventually becomes a tremendous challenge, since the blockchain stores the records of all transactions back to the origin. According to IBM developers, sidechains, treechains, and mini-blockchains may be used to address the problem [27].

Peer-list: the blockchain can store the history of a smart object, but it is not designed to recognize the objects themselves. Therefore, a peer-list is required. After an object ID has been recognized, such ID can be used to browse the blockchain.

Single Points of Failure: malicious users can exploit undisclosed or unknown vulnerabilities of the exchange nodes' code and potentially bring down the whole network.

Privacy: all the nodes of the blockchain network have access to each others' transactions, so privacy is not guaranteed.

VI. DEPLOYMENT OF BLOCKCHAINS FOR THE IOT: ISSUES AND CONCERNS

The development of blockchains, cryptocurrencies and smart contracts for the IoT still entails several issues and concerns, at a technical and societal level.

Privacy. In the blockchain, privacy and confidentiality still constitute a problem, since all the nodes of the network have access to each others data, and transactions are also visible to those who explore the blockchain [17] [21] [29] [30]. To overcome this issue, participants may use different addresses when sending or receiving transactions [30]. Other methods such as homomorphic encryption and zero-knowledge proof are also effective, insofar they make transaction inputs visible to senders and recipients only, still enabling all other nodes of the network to verify the transaction validity [30]. These techniques, however, may prove to be time-consuming, unpractical or not optimized for the IoT resource-constrained environment [17]. Enigma developers have proposed the best solution so far, through off-chain data storage and secure Multi Party Computation

(sMPC). This platform is very promising and it represents a good example of *privacy-by-design*.

Smart contracts limits. Smart contracts have limited legal enforceability, and disputes may occur. This issue can be prevented or mitigated through a “dual integration”, namely embedding a reference to a real world contract into the smart contract, and vice versa [17] [31]. Since smart contracts are deterministic, potentially unstoppable and not editable once running, participants should also embed fail-safe expedients in the code to mitigate possible negative effects – e.g. to recover funds in case of errors [17].

Expected value of tokens. To redeem a token gained exchanging assets in blockchain transactions or smart contracts may turn out to be problematic. Participants should be aware of the effective value of tokens, before trading [17].

Potential risk of hyper-tokenization. Both Enigma platform and IOTA allow micro-payments and monetization of user-generated data. They transform users from being passive and often unwitting sources of personal data for third parties, to pro-active subjects who own their data and gain a benefit from them. Nonetheless, if a myriad of new generation blockchains and cryptocurrencies with similar features will be created in future, the ubiquitous diffusion of micro-payments combined with the pervasiveness of the IoT may easily lead to an hyper-tokenization of society. The risk is to create a “digital feudalism” [31], where all human activities are monetized and/or controlled by corporations. This paradigm is clearly advocated by IBM in the *Economy of Everything* and it may result in unpredictable, dystopian social effects, since it may change, for example, the spontaneity or gratuity of our behaviors.

Platforms and technocracy. Practice shows that the implementation of blockchains in the IoT ecosystem increasingly takes place in global platforms, leveraged by big IT corporations. They aim at becoming global intermediaries between clients and blockchain protocol providers, using blockchain -as- a-service (BaaS) to attract more clients in their cloud computing portfolio. While corporations pursue their own legitimate commercial interests, we cannot overlook the fact that they will increasingly play a major role in the IoT industry, with possible new forms of centralization at global level. The transition to Internet Protocol version 6 (Ipv6) as IP addressing standard is likely to exacerbate the problem, since it allows the deployment of the IoT on a very large scale, with the assignation of a unique address to an endless number of objects. Again, this can easily transform every dimension of our daily live into transactions occurring in big corporations' platforms. Some scholars deplored the implications of such scenario, considered as one of the “Trojan horses” of a technocratic global transformation that is already affecting every aspect of our existence [33].

VII. CONCLUSION

The blockchain technology has great potential for driving the next wave of innovation in the IoT and it can promote the emergence of new business models, significantly modifying the existing systems and processes [17]. Possible effects of implementation, however, should take account of specific contexts of use. The case studies examined, indeed, lead us to very different conclusions about overall benefits and drawbacks of a blockchain-based IoT for society as a whole.

On one side, platforms such as Enigma respond very appropriately to the issue of users privacy, and they can hopefully be implemented as a best practice in the industry. On the other side, however, the deployment of the blockchain within global, centralized platforms does not mitigate the possible dystopian effects of the IoT – which remains a “wicked problem”. In particular, a wide dissemination and use of smart contracts and digital tokens as seamless micro-payment systems should be carefully measured against an anthropological and social dimension of technological innovation, building opportune safeguards against their potentially intrusive, materialistic and deterministic nature.

The French philosopher and urbanist Paul Virilio wrote in an essay: “When you invent the ship, you also invent the shipwreck ... Every technology carries its own negativity, which is invented at the same time as technical progress” [34]. This effective metaphor gives us a vivid understanding of the very nature of the IoT, when it is powered by blockchains, smart contracts and cryptocurrencies. Cross-disciplinary research and informed debate between all relevant stakeholders is therefore particularly necessary, to find a balance between need for innovation and social sustainability.

ACKNOWLEDGMENT

The author would like to thank Gregor Boroša for his valuable comments and suggestions.

REFERENCES

- [1] Recommendation ITU-T Y.4000/Y.2060. (Jun. 2012). Overview of the Internet of things. [Online]. p.1. Available: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>
- [2] M. Weiser,, R. Gold, and J. Brown. (1999). The origins of ubiquitous computing research at PARC in the late 1980s [Online]. *IBM Syst. J.*, 38 (4), pp. 693-696, 1999. Available: [doi:10.1147/sj.384.0693](https://doi.org/10.1147/sj.384.0693)
- [3] M. Weiser,, R. Gold, and J. Brown. (1999). The origins of ubiquitous computing research at PARC in the late 1980s. [Online]. *IBM Syst. J.*, 38 (4), pp. 694, 1999. Available: [doi:10.1147/sj.384.0693](https://doi.org/10.1147/sj.384.0693)

- [4] M. Chen, J.Wan, and F. Li. (2012). Machine-to-Machine Communications: Architectures, Standards and Applications. [Online]. *KSII Transaction on Internet and Information Systems*, 6 (2). Available: <https://www.researchgate.net/publication/264846553>
- [5] BCS – The Chartered Institute for IT. (2013, Feb.). “The Societal Impact of the Internet of Things”. [Online]. Available: <http://www.theinternetofthings.eu/sites/default/files/%5Buser-name%5D/The%20Societal%20Impact%20of%20the%20Internet%20of%20Things.pdf>
- [6] Borgohain T., Kumar U., and Sanyal S. (2015) Survey of Security and Privacy Issues of Internet of Things. [Online]. Available: <https://arxiv.org/abs/1501.02211>
- [7] J. Sánchez Alcón, L. López, J. Martínez, J. and G. Rubio Cifuentes. (2015). Trust and Privacy Solutions Based on Holistic Service Requirements. [Online]. *Sensors*, 16(1), p.1. Available: <http://www.mdpi.com/1424-8220/16/1/16>
- [8] R. H. Weber. (2015). Internet of things: Privacy issues revisited. [Online]. *Computer Law & Security Review*. 31 (5), pp. 618-627. Available: https://www.researchgate.net/publication/283758467_Internet_of_things_Privacy_issues_revisited
- [9] J. Ziegeldorf, O. Morchon, and K. Wehrle. (2013). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), pp. 2728-2742. Available: <https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf>
- [10] M. Langheinrich. (2001, September). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. Presented at International conference on Ubiquitous Computing [Online]. Available: <http://cs.gmu.edu/~jpsousa/classes/699/papers/privacy%20Langheinrich.pdf>
- [11] E. Goodman. (2015). The Atomic Age of Data: Policies for the Internet of Things. [Online]. *SSRN Electronic Journal*. Available: <http://ssrn.com/abstract=2605201>
- [12] Spiekermann S., and Cranor L.F.(2009). Engineering Privacy. [Online]. *IEEE Trans. Software Eng.*, 35 (1), pp. 67–82. Available: <http://ec-wu.at/spiekermann/publications/Engineering%20Privacy.pdf>
- [13] S. Gurses, and J.M. Del Alamo. (Mar, 2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice. [Online] *IEEE Security and Privacy Magazine*. Available: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7448344>
- [14] A. Cavoukian. (2011) Privacy by Design—The 7 Foundational Principles. [Online]. Available: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
- [15] R. H. Weber. (2010). Internet of Things—New security and privacy challenges. [Online]. *Computer Law & Security Review*, 26(1), pp. 23-30. Available: <http://www.sciencedirect.com/science/article/pii/S0267364909001939>
- [16] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [17] K. Christidis, and M. Devetsiokiotis. Blockchains and Smart Contracts for the Internet of Things. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=7467408
- [18] M. Swan, *Blockchain: Blueprint for a New Economy*. 2015. O'Reilly Media, Inc. pp. x-xiii
- [19] N. Szabo. (1999). Smart contracts. [Online]. Available: <http://szabo.best.vwh.net/smart.contracts.html>
- [20] M. Swan, *Blockchain: Blueprint for a New Economy*. 2015. O'Reilly Media, Inc. pp. pp. 16-19
- [21] G. Zyskind, O. Nathan, and A. Pentland (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. [Online]. *IEEE Security and Privacy Workshops (SPW)*, pp.180–184. Available: <http://web.media.mit.edu/~guyzys/data/ZNP15.pdf>
- [22] G. Zyskind, O. Nathan, and A. Pentland. (2015). Enigma: Decentralized Computation Platform with Guaranteed Privacy. [Online]. Available: <http://arxiv.org/pdf/1506.03471v1.pdf>
- [23] J. P. Buntinx. (2016) IOTA: Internet of Things Without the Blockchain? [Online] *Bitcoinist.net*. Available: <http://bitcoinist.net/iota-internet-things-without-blockchain/>
- [24] S. Popov. (2016) The tangle. [Online] Available: http://www.iotatoken.com/IOTA_Whitepaper.pdf
- [25] Bitcoinist.net. The Vanbex Report: The Tangle and the Blockchain. [Online]. Available: <http://bitcoinist.net/vanbex-report-tangle-blockchain/>
- [26] P. Rizzo. (2016) Why Microsoft Wants 'Every Blockchain' on its Azure Platform. [Online]. Available: <http://www.coindesk.com/microsoft-blockchain-azure-marley-gray/>
- [27] IBM. (2015). ADEPT: An IoT Practitioner Perspective - DRAFT COPY FOR ADVANCE REVIEW. [Online]. Available: https://archive.org/stream/pdfyesMcC00dKmdo53-/IBM%20ADEPT%20Practitioner%20Perspective%20-%20Pre%20Publication%20Draft%20-%202015Jan%202015_djvu.txt
- [28] IBM Institute for Business Value. (2015). Device democracy. Saving the future of the Internet of Things. [Online]. Available: <http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/>
- [29] M. Signorini. (2015) Towards an internet of trust: issues and solutions for identification and

authentication in the internet of things. [Online]. Ph.D. Dissertation. Univ. Pompeu Fabra. Dep. de Tecnologies de la Informació i les Comunicacions. Available: <http://hdl.handle.net/10230/25746>

- [30] G. Greenspan. (Jul. 2015). MultiChain Private Blockchain — White Paper. [Online]. Available: <http://www.multichain.com/download/MultiChain-White-Paper.pdf>
- [31] Eris Industries - eris:legal. [Online]. Available: <https://erisindustries.com/components/erislegal/>
- [32] B. Sterling, *The Epic Struggle of the Internet of Things*. New York: Strelka Press, 2014.
- [33] P. M. Wood, *Technocracy Rising*. The Trojan Horse of Global Transformation. Mesa, Ariz.: Coherent Publishing, 2015, pp. 145-147
- [34] P. Virilio, P. Petit, and S. Lotringer, *Politics of the Very Worst*. New York: Semiotext(e), 1999.



Marcella Atzori is a political analyst and academic researcher specialized in technopolitics and global affairs, currently affiliated with the University College of London, Center for Blockchain Technologies. She holds a master degree in political science, a Ph.D in international politics and a master degree in digital currency from the University of Nicosia, Cyprus. As a blockchain and digital currency specialist, Dr. Atzori advises governments, institutions, SMEs, academic communities, media, and other relevant actors on these issues.